

ABSTRACT

A method and apparatus for securing networks, focusing on application in Fibre Channel networks. A combination of unique security techniques are combined to provide overall network security. Responsibility for security in the network is assigned to one or more designated entities. The designated entities deploy management information throughout the network to enhance security by modifying the capabilities and operational permissions of the devices participating in the network. For example, through network control: logical management access or physical I/O access may be limited on a per device or per I/O basis; and all devices and ports in the network operate only with other approved devices and ports. These designated entities can better manage network security by exploiting a unique link authentication system as well as a unique push-model secure distributed time service. The link authentication involves a multi-phase nonce exchange exploiting various derivations of the nonce and other information such as hashes and encryptions. The push-model secure time distribution departs from the traditional Fibre Channel pull mode time distribution and provides for secure and reliable distributed time so that various security attacks may be defeated.